

Enterprise Security Gateway VPN Requirements

VPN Tunnel Specifications

To establish and operate an access VPN service to the Enterprise Security Gateway (ESG), Non-FAA external users must comply with FAA security requirements for the connection, as well as be compatible with security gateway equipment. IPSec encompasses a suite of protocols; however, the FAA reserves the right to dictate particular choices to meet best practices and security mandates. In general, to establish extranet services users must meet the following requirements:

- Employ a site-to-site VPN Tunnel. Client based VPN solutions are not accepted. Moreover, the FAA provides no external user hardware or software to support VPNs.
- Provide one or more fixed public IP addresses for the External User's VPN concentrator.
- The Enterprise Security Gateway requires each External user to use a separate IP address, to communicate with each NAS program; i.e., if the user needs to communicate with two programs/systems, it will need to use two separate IP addresses on its side.
- Comply with standard Enterprise Security Gateway access VPN service / IPSec settings:
 - Encapsulation Security Payload (ESP)
 - Encryption: AES-256
 - Authentication: SHA-1
 - IPSec / IKE Authentication: Pre-shared secret and digital certificate
 - IKE: Version 1
 - IKE phase 1: Diffie-Hellman group 5
 - Perfect Forward Secrecy (PFS): Diffie-Hellman group 1
 - Pre-shared secret key (to be exchanged at the time of VPN establishment)

Note: The Enterprise Security Gateway does not use simplified mode, aggressive mode or VPN communities for external user access VPN tunnels.

- Conservatively configure security settings to permit only the required application traffic. The IP source, destination, and ports detail must be fully specified.

Example:

<i>Client source IP</i>	<i>x.x.x.x</i>
<i>Destination IP (Server):</i>	<i>y.y.y.y</i>
<i>Destination TCP Port:</i>	<i>3000</i>

Equipment Compatibility

All external user access VPN tunnels created between the FAA and external end-user systems are based on IPSec. Vendor implementation variances could result in compatibility problems even though IPSec is an open suite of standards (see RFC 2401 for general information).

IMPORTANT NOTE: You should check that the product selected meets the minimum VPN Technical Requirements specified earlier in this document.